REMARKS

In the Office Action dated March 8, 2007 the Examiner has rejected the pending claims 1-16 and 18-44. More specifically, the Examiner has repeated and made final the rejection of claims 1-9, 16, 19-24, 31-38 and 41-44 under 35 USC 103(a) as being unpatentable over Tamaki et al. (US2003/0054796) in view of Dahan et al. (US2004/0123118); the Examiner has repeated and made final the rejection of claims 10-11, 25-26, and 39-40 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Kirkup (US20040142686); the Examiner has repeated and made final the rejection of claims 12,13, 27 and 28 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Sakakura (JP2002209028); the Examiner has repeated and made final the rejection of claims 14 and 29 under 35 USC 103(a) over Tamaki in view of Dahan, Sakakura and in further view of Piazza (US2003/0061358); and the Examiner has repeated and made final the rejection of claims 15 and 30 are rejected under 35 USC 103(a) as being unpatentable over Tamaki in view of Dahan, Sakakura and in further view of Von Kaenel (US20040117358). Respectfully, the rejection is traversed below.

Claims 21-30 are canceled. Claim 6 is amended for clarification. Support for the amendment can be found at least on page 9, lines 1-10. Claims 1, 3-5, 8, 16, 18-20, 31, 33, 35, 37, 41, and 43 have been amended to remove certain subject matter from the claims. Claim 2 has been amended to correct a typographical error previously unnoticed. Claims 45-47 has been added. Support for these new claims can be found at least on page 7, line 19, to page 9, line 30. No new matter is added.

In the rejection that includes all of the independent claims 1, 16, 31, 35, 41 and 43 the Examiner again acknowledges that Tamaki et al. does not teach the use of trusted software, and states that this limitation is taught by Dahan in paragraph [0011]. The Examiner further states that it would have been obvious to apply the teachings of Dahan to Tamaki in order to "to improve security for the network".

It is respectfully submitted that this rejection is a clear error on the part of the Examiner.

In the paragraph [0011] cited by the Examiner what Dahan actually discloses is the following:

> A secure execution mode is thus provided on a platform where the only trusted software is the code stored in on-chip ROM. An indicator means observable by a user of the digital system is provided, wherein the indicator means can only be activated by the trusted program code while in the secure mode of operation.

To place this paragraph in context, Dahan discloses in paragraph [0009] a security limitation of the prior art:

> On a smart device enabled for a secure class of applications such as for m-commerce (mobile commerce) or e-banking (electronic banking), the user is asked to enter secret information such as a password on the keyboard or to sign messages displayed on the screen. When doing so, the user has no other choice then to fully rely on the integrity of his device. However, there is no way for the user to detect that a hacker or a virus has defeated the security framework of his device.

Dahan continues "Thus, improvements in system security are needed" (paragraph [0010]), and further discloses that "In general, and in a form of the present invention, a digital system is provided with a secure mode (3rd level of privilege) built in a non-invasive way on a processor system" (paragraph [0011]).

Dahan continues in paragraph [0022]:

> In secure mode, the access to a physical user interface such as a keyboard or display are restricted to secure applications through trusted drivers ... Otherwise, if a virus/hacker manages to download a forged driver on the smart device, then the user has no way to know that he cannot rely on his device.

In addition, the "ROM is partitioned in two parts: a secure portion of the ROM that is protected by the secure bit and can only be accessed in secure mode; and a public portion of the ROM that is always accessible and contains the boot area" (par. [0054])" Therefore, "The secure mode is entered when security signal 302 is asserted" and "In secure mode, CPU 200 can only execute

code that is stored in secure ROM 310 or secure SRAM 312" (par. [0053]).

A method is disclosed in Dahan "for protecting sensitive information from access by non-trusted software" and to provide that "There can exist no possible flows by which non-trusted code can either fool the hardware into entering secure Mode, or get trusted code to perform tasks it shouldn't." (paragraphs [0044] and [0045]). Dahan thus clearly discloses a technique to restrict access to, and prevent tampering with a digital device.

As was noted above, in the office action the Examiner acknowledges that Tamaki does not teach the use of trusted software. However, it has been clearly shown that Dahan uses a hardware implementation to secure a digital device (paragraphs [0022] and [0044]). Therefore, even if the "secure execution mode" of Dahan were incorporated into at least one of the end user terminals 111-114 and into the personal communications providers terminals 115-117 of Tamaki et al., which is not admitted is suggested, **the resulting modified terminals would appear to simply facilitate a secure mode on the terminal itself** (Dahan paragraphs [0044] and [0045]). Clearly, there is no suggestion in such a proposed modification that there would be executed, as claim 1 recites in part:

> **establishing a service provisioning relationship between the user device and a bridging user device;**
> providing a desired service for the user device with the service provider via the bridging user device;
> while providing the service, **recording charging data for the service provisioning relationship** between the user device and the bridging user device; and
> reporting the charging data from the bridging user device to the service provider, where at least **establishing and recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device.**

Thus, for the reasons stated Tamaki in view of Dahan does not disclose or suggest claim 1. That is, at least for the reason that if the proposed combination of Tamaki and Dahan were made, at most the terminals of Tamaki would be operational in a "secure mode" so that "access to a

physical user interface such as a keyboard or display are restricted to secure applications through trusted drivers" (Dahan at paragraph [0022]). Without expressly or impliedly admitting that the proposed combination is suggested, clearly the proposed combination would not render obvious at least the subject matter that is highlighted above for claim 1.

In the **Response to Arguments** section of the most recent office action the Examiner states that in the previous argument the applicant submitted that Tamaki and Dahan do not teach "establishing a service provisioning relationship between the user device and a bridging user device through a first wireless network", and refers to Tamaki et al. at paragraph [0031]. The Examiner has further stated that in the previous argument the applicant submitted that Tamaki and Dahan do not teach "recording charging data for the service provisioning relationship between the user device and the bridging user device", and refers to Tamaki et al. in Figure 4 and paragraph [0033].

It is respectfully submitted that the Examiner has referred to only a portion of the previous arguments. What the applicant argued, as outlined above, was that the proposed combination of Tamaki et al. and Dahan et al. does not expressly teach or suggest "**establishing a service provisioning relationship** between the user device and a bridging user device through a first wireless network", or "**recording charging data for the service provisioning relationship** between the user device and the bridging user device", where "**at least establishing and recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device**".

The Examiner then continues in the **Response to Arguments** by stating that the applicant submitted that Tamaki and Dahan do not teach ".. establishing and recording use trusted software...", and refers to the paragraph [0011] of Dahan et al. where "Dahan teaches the use of trusted software".

As was argued in the prior response, at most what Dahan et al. teach is a technique to secure a portion of a digital device via a hardware implementation (paragraphs [0022] and [0044]). Thus,

even if the "secure execution mode" of Dahan were incorporated into at least one of the end user terminals 111-114 and into the personal communications providers terminals 115-117 of Tamaki et al., which is not admitted is suggested, **the resulting modified terminals would appear to simply facilitate a secure mode on the terminal itself** (Dahan paragraphs [0044] and [0045]). Thus, when read in context the paragraph [0011] as cited by the Examiner in Dahan discloses only the following:

> A secure execution mode is thus provided on a platform where the only trusted software is the code stored in on-chip ROM. An indicator means observable by a user of the digital system is provided, wherein the indicator means can only be activated by the trusted program code while in the secure mode of operation.

There is clearly no suggestion or disclosure of at least the following subject matter of independent claim 1:

> "**establishing a service provisioning relationship** between the user device and a bridging user device"... "**recording charging data for the service provisioning relationship** between the user device and the bridging user device", where "**at least establishing and recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device**".

It is further noted that in the rejection of claim 6 the Examiner states that Tamaki teaches the method as in claim 1 citing "figures 3 & 5 and paragraphs [0031]-[0033], [0035]." Respectfully the applicant disagrees with the Examiner.

Claim 6 recites:

> "A method as in claim 1, where establishing includes negotiating the specifics of charging for the service provisioning relationship between the user device and the bridging user device using an offer-counteroffer technique."

In the reference cited by the Examiner, Tamaki et al. disclose "The end users and personal

communications service providers pay three types of fees according to the bill from the communications service provider: a utilization fee for communications service provider, a utilization fee for information service provider and a utilization fee for personal communications service provider" (par. [0033]). In addition, Tamaki et al. disclose that "In order to receive low-priced communications service offered by the ad hoc network of terminals with repeater function owned by personal communications service providers, the end users and personal communications service providers take the registration procedure for personal communications service provider and make a contract to pay a monthly fee based on the flat rate system to the communications service provider" (par. [0035]). Thus, Tamaki et al. do not disclose " negotiating the specifics of charging for the service provisioning relationship between the user device and the bridging user device using an offer-counteroffer technique," as claim 6 recites in part.

Tamaki et al. merely disclose that the users can agree to contract on a monthly basis to receive a discount (par. [0035]). Clearly, Tamaki et al. does not disclose or suggest any negotiation of the charging specifics as in claim 6, in particular a negotiation between a user device and a bridging user device.

In addition, for at least the reasons stated above Tamaki et al. in view of Dahan et al. does not disclose or suggest, as claim 16 recites in part:

> "where said user device, said bridging user device and said service provider execute computer code **to establish a service provisioning relationship between said user device and said bridging user device**.."**to record charging data for the service provisioning relationship** between said user device and said bridging user device"..."where said computer code comprises trusted software comprising a certified unit of code running on said user device and on said bridging user device.".

In addition, for at least the reasons stated above Tamaki et al. in view of Dahan et al. does not disclose or suggest, as claim 31 recites in part:

> "said memory storing computer code executable by said data processor to request

> a service to be provided by a service provider and to **establish a service provisioning relationship between said mobile device and another device**...where **said computer code comprises trusted software comprising a certified unit of code running on said mobile device and on said another device**...".

In addition, for at least the reasons stated above Tamaki et al. in view of Dahan et al. does not disclose or suggest, as claim 35 recites in part:

> "said memory storing computer code executable by said data processor to **establish a service provisioning relationship between said mobile device and another device** through said first network, said computer code **comprising trusted software comprising a certified unit of code running on said mobile device and on said another device...**"

In addition, for at least the reasons stated above Tamaki et al. in view of Dahan et al. does not disclose or suggest, as claim 41 recites in part:

> "..said data processor operating to request a service to be provided by a service provider and to **establish a service provisioning relationship between said mobile terminal and a device through said first network**, ...where said **data processor operates under control of trusted software comprising a certified unit of code stored in said mobile terminal and in said device**..".

In addition, for at least the reasons stated above Tamaki et al. in view of Dahan et al. does not disclose, as claim 43 recites:

> "said **data processor operable to establish a service provisioning relationship between said mobile terminal and a device through said first network**.... where said **data processor is further operable to record charging data for the service provisioning relationship between said mobile terminal and said device, and to report the charging data to said service provider** over said second network, **where said data processor operates under control of trusted software comprising a certified unit of code stored in said mobile terminal and in said device**".

In that Tamaki in view of Dahan does not disclose or suggest the subject matter found in claims

1, 6, 16, 31, 35, 41 and 43; and all the claims 1, 6, 16, 31, 35, 41 and 43 should be allowed.

The Examiner rejects claim 14 under 35 USC 103(a) over Tamaki in view of Dahan, Sakakura and in further view of Piazza. Respectfully the applicant disagrees.

The Piazza reference cited by the Examiner states: "To prevent the transmission of clear text passwords and to secure information, all transactions including the initial password exchange are encrypted with, for example, SSL (Secure Sockets Layer) 3.0. 128-bit encryption" (par. [0150]). However, the Examiner has failed to consider whether Dahan would function when "all transactions including the initial password exchange are encrypted with, for example, SSL (Secure Sockets Layer) 3.0. 128-bit encryption" as Piazza discloses.

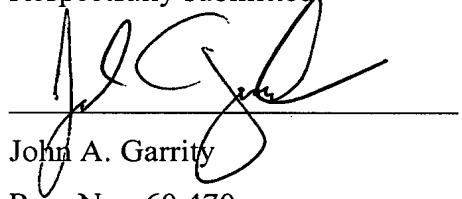
Dahan discloses "The security state machine monitors various signals 330 from processor 200's external interfaces and in particular, the addresses fetched by the processor on the instruction bus" (par. [0052]). Further, "The security state machine is tightly coupled to low-level assembly code from the entry sequence" and "It reacts to events generated by the entry sequence on the monitored signals" (par. [0052]). There is no disclosure in Dahan to indicate that the Security State Machine would be able to process "all transactions including the initial password exchange ... encrypted with, for example, SSL (Secure Sockets Layer) 3.0. 128-bit encryption" as Piazza discloses. As Dahan discloses a method "for protecting sensitive information from access by non-trusted software," it would appear to be counter to this method to allow an unreadable encrypted data stream to access the secured device in Dahan. Dahan does not disclose or suggest that "all transactions including the initial password exchange" encrypted using SSL 128-bit encryption would be allowed access to the digital device in Dahan. As claim 14 recites this feature; the reference Tamaki in view of Dahan, Sakakura and in further view of Piazza does not disclose, teach or suggest claim 14; and claim 14 should be allowed.

Further, for at least the reasons already stated the references cited are not seen to disclose or suggest claim 45. Thus, claim 45 should be allowed.

The applicant again provides notice that the indicated allowability of the claims for these reasons alone should not be construed as an acknowledgment that the Applicant is in agreement with the Examiner's other reasons for rejecting the claims based variously on Tamaki and the other cited documents.

The Examiner is respectfully requested to reconsider and remove the rejections of the claims, and to allow all of the pending claims 1-16, 18-20, and 31-47 as now presented for examination. An early notification of the allowability of claims 1-16, 18-20, and 31-47 is earnestly solicited.

Respectfully submitted,



6/8/07

John A. Garrity
Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

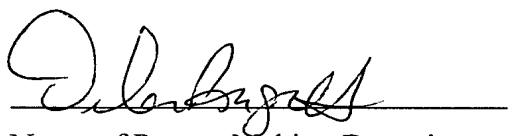
Date

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

June 8, 2007

Date



Name of Person Making Deposit